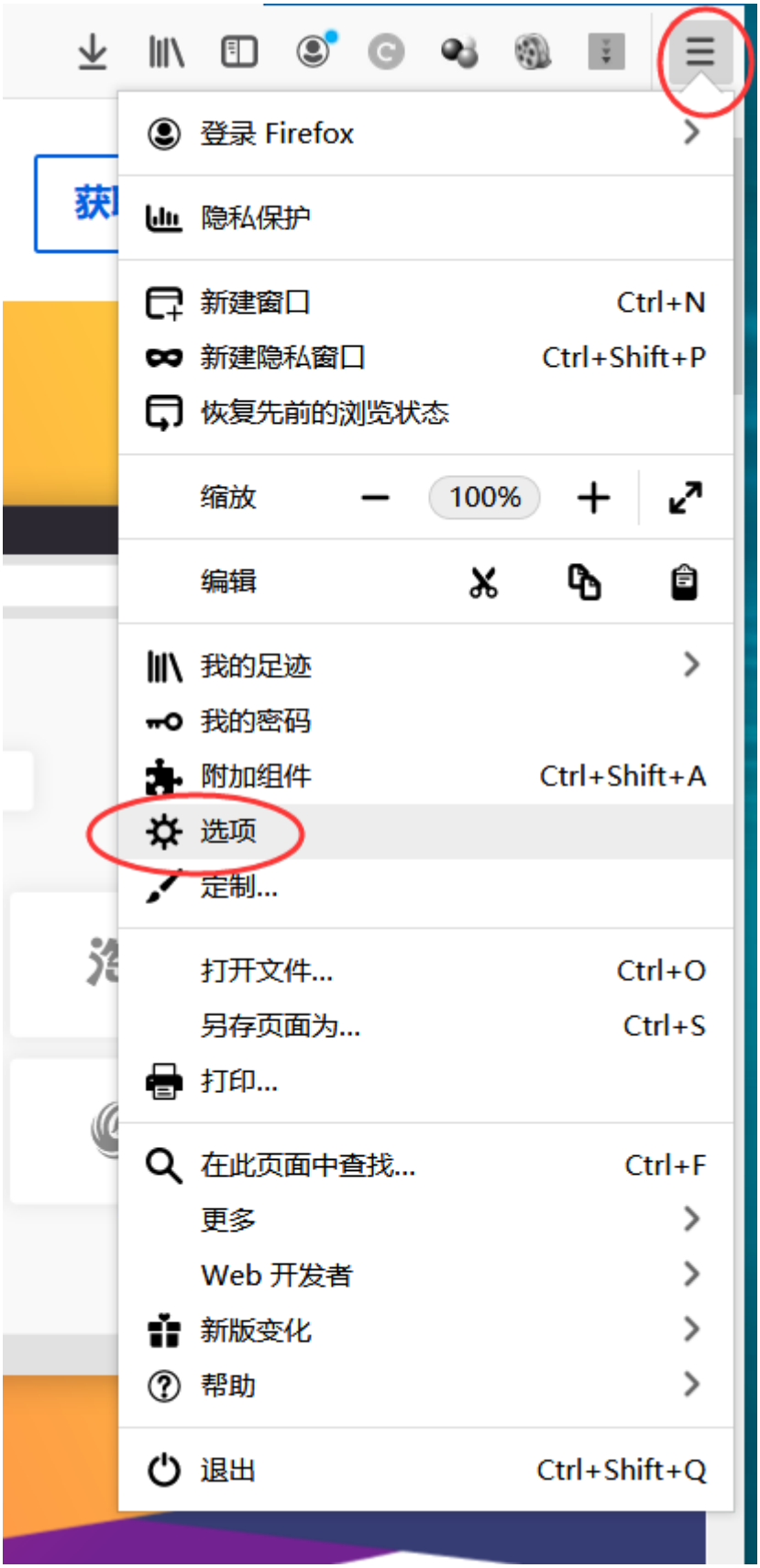
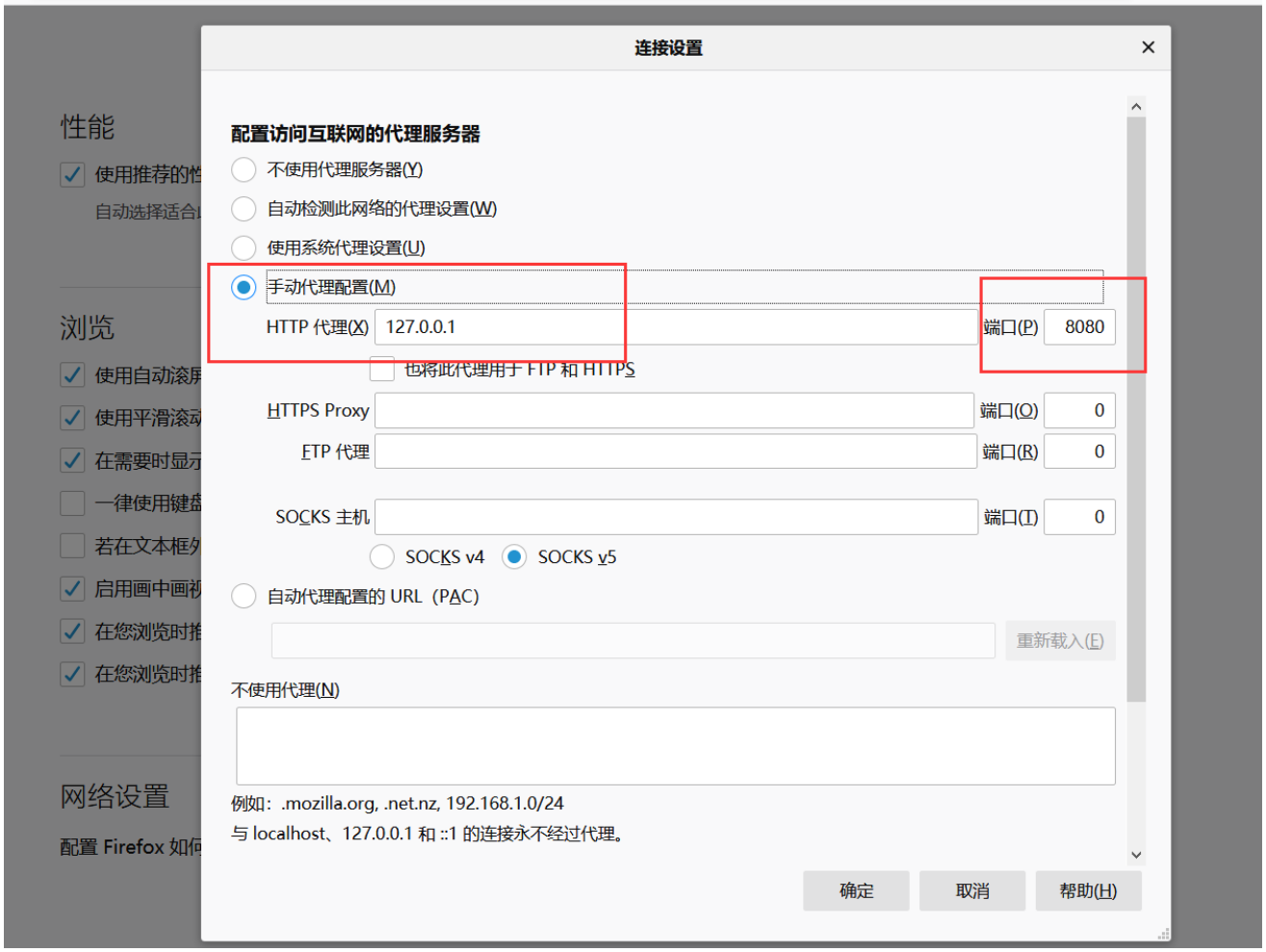
步骤1：浏览器设置代理

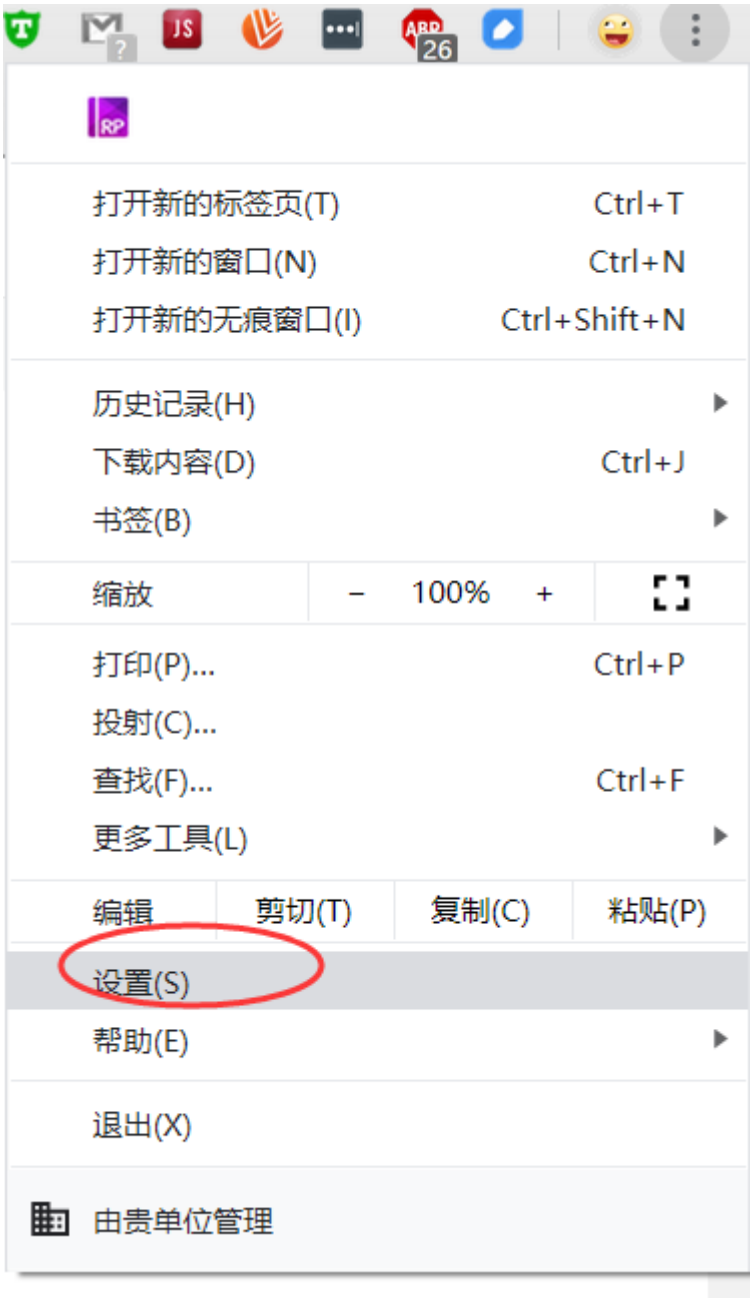
推荐火狐浏览器

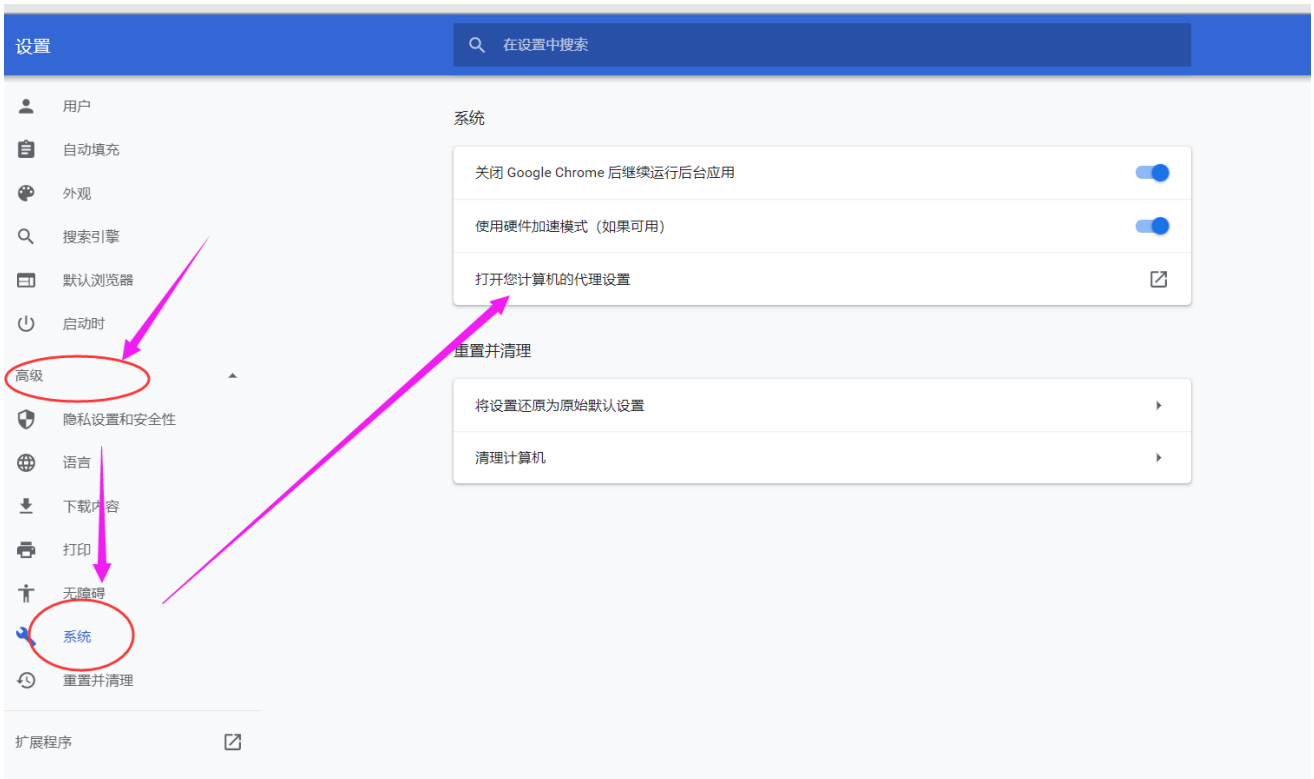

登录 Firefox
隐私保护
新建窗口 Ctrl+N
新建隐私窗口 Ctrl+Shift+P
恢复先前的浏览状态
缩放 100%
编辑
我的足迹
我的密码
附加组件 Ctrl+Shift+A
选项
定制...
打开文件... Ctrl+O
另存页面为... Ctrl+S
打印...
在此页面中查找... Ctrl+F
更多
Web 开发者
新版变化
帮助
退出 Ctrl+Shift+Q


在选项中查找
常规
主页
搜索
隐私与安全
同步
性能
使用推荐的性能设置(U) 详细了解
自动选择适合此电脑配置的设置。
浏览
使用自动滚屏(A)
使用平滑滚动(M)
在需要时显示触摸键盘(K)
一律使用键盘方向键浏览网页（键盘浏览模式）(C)
若在文本框外输入，则在页面中查找文本(X)
启用画中画视频控件(E) 详细了解
在您浏览时推荐扩展(R) 详细了解
在您浏览时推荐新功能(F) 详细了解
网络设置
扩展和主题
配置 Firefox 如何连接互联网。 详细了解
设置...(E)


连接设置
配置访问互联网的代理服务器
不使用代理服务器(Y)
自动检测此网络的代理设置(W)
使用系统代理设置(U)
手动代理配置(M)
HTTP 代理(X) 127.0.0.1
端口(P) 8080
也将此代理用于 FTP 和 HTTPS
HTTPS Proxy
端口(O) 0
FTP 代理
端口(R) 0
SOCKS 主机
端口(T) 0
SOCKS v4
SOCKS v5
自动代理配置的 URL（PAC）
重新载入(E)
不使用代理(N)
例如：.mozilla.org, .net.nz, 192.168.1.0/24
与 localhost、127.0.0.1 和 ::1 的连接永不经过代理。
确定
取消
帮助(H)

chrome浏览器

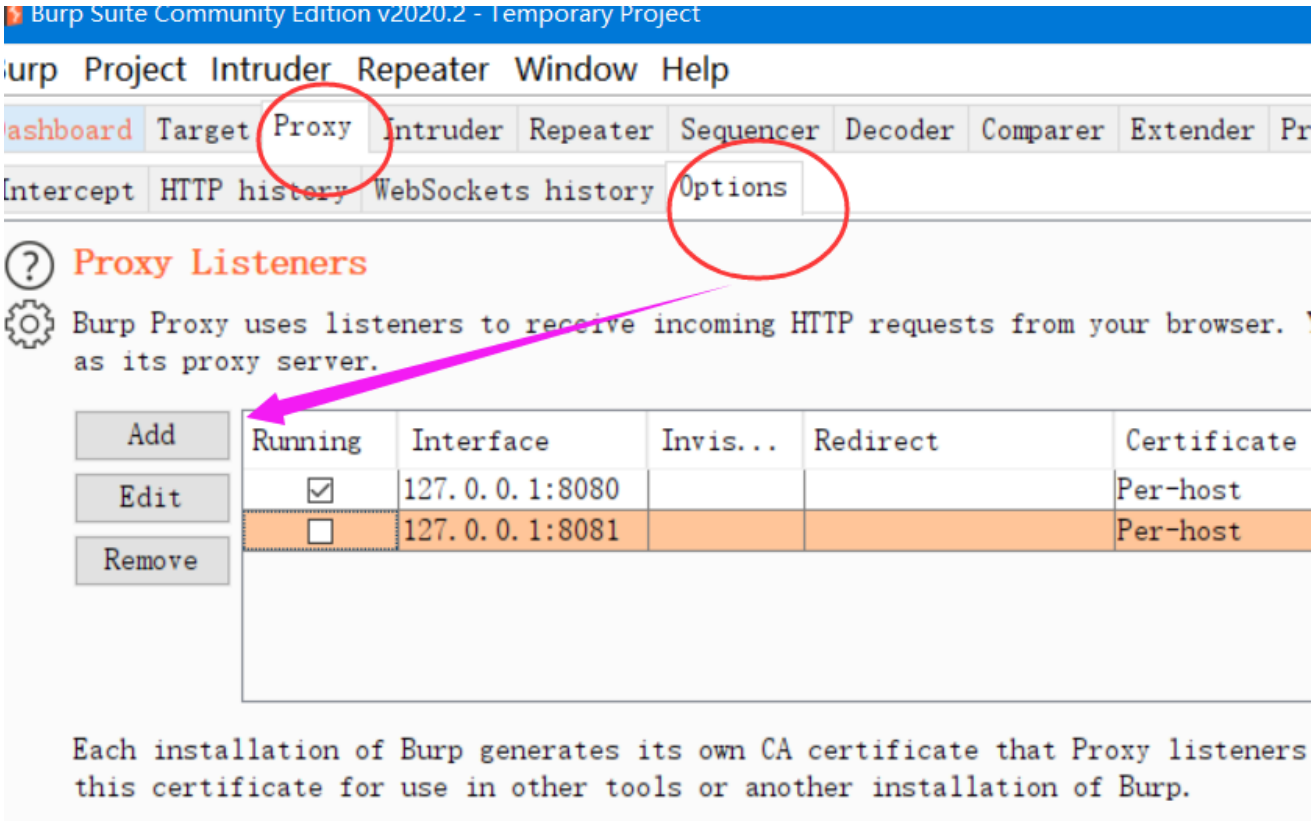

JS
ABP
26
RP
打开新的标签页(T) Ctrl+T
打开新的窗口(N) Ctrl+N
打开新的无痕窗口(I) Ctrl+Shift+N
历史记录(H)
下载内容(D) Ctrl+J
书签(B)
缩放 – 100% +
打印(P)... Ctrl+P
投射(C)...
查找(F)... Ctrl+F
更多工具(L)
编辑 剪切(T) 复制(C) 粘贴(P)
设置(S)
帮助(E)
退出(X)
由贵单位管理

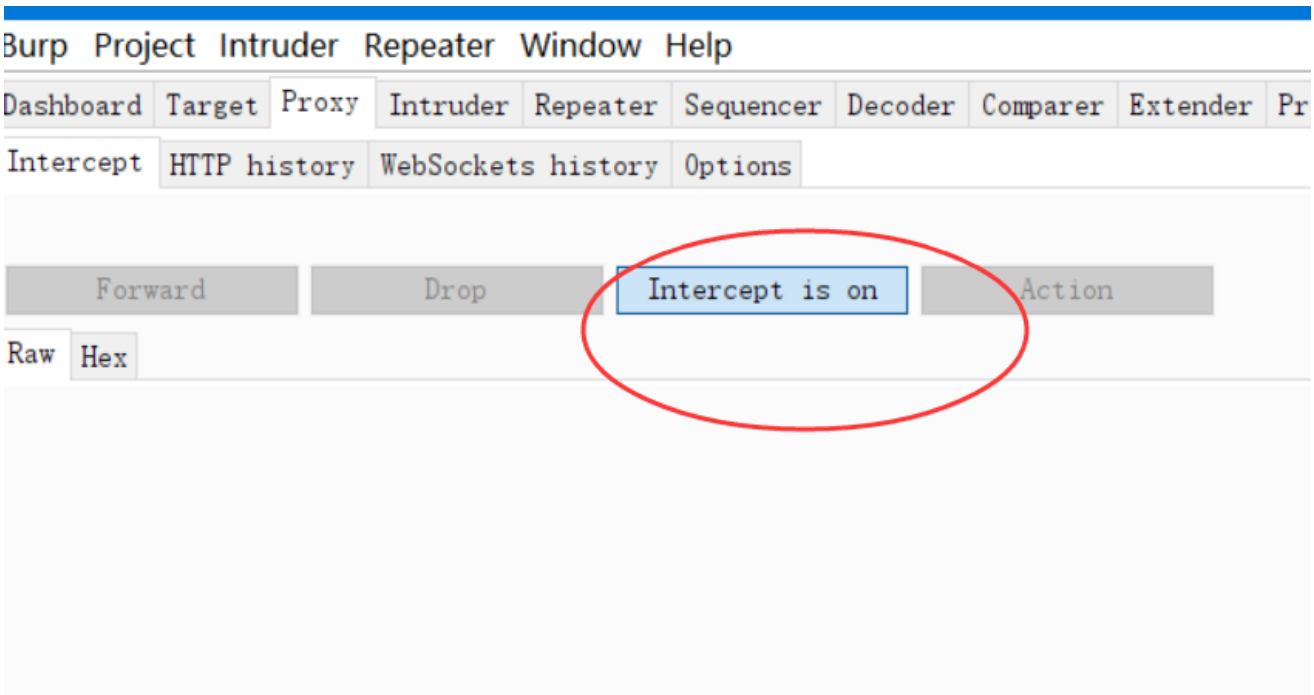

设置
在设置中搜索
用户
自动填充
外观
搜索引擎
默认浏览器
启动时
高级
隐私设置和安全性
语言
下载内容
打印
无障碍
系统
重置并清理
扩展程序
系统
关闭 Google Chrome 后继续运行后台应用
使用硬件加速模式（如果可用）
打开您计算机的代理设置
重置并清理
将设置还原为原始默认设置
清理计算机


Internet 属性
常规
安全
隐私
内容
连接
程序
高级
要设置 Internet 连接，单击"设置"。
设置(U)
拨号和虚拟专用网络设置
VPN 连接
添加(D)...
添加 VPN(P)...
删除(R)...
如果要为连接配置代理服务器，请选择"设置"。
设置(S)
局域网(LAN)设置
LAN 设置不应用到拨号连接。对于拨号设置，单击上面的"设置"按钮。
局域网设置(L)

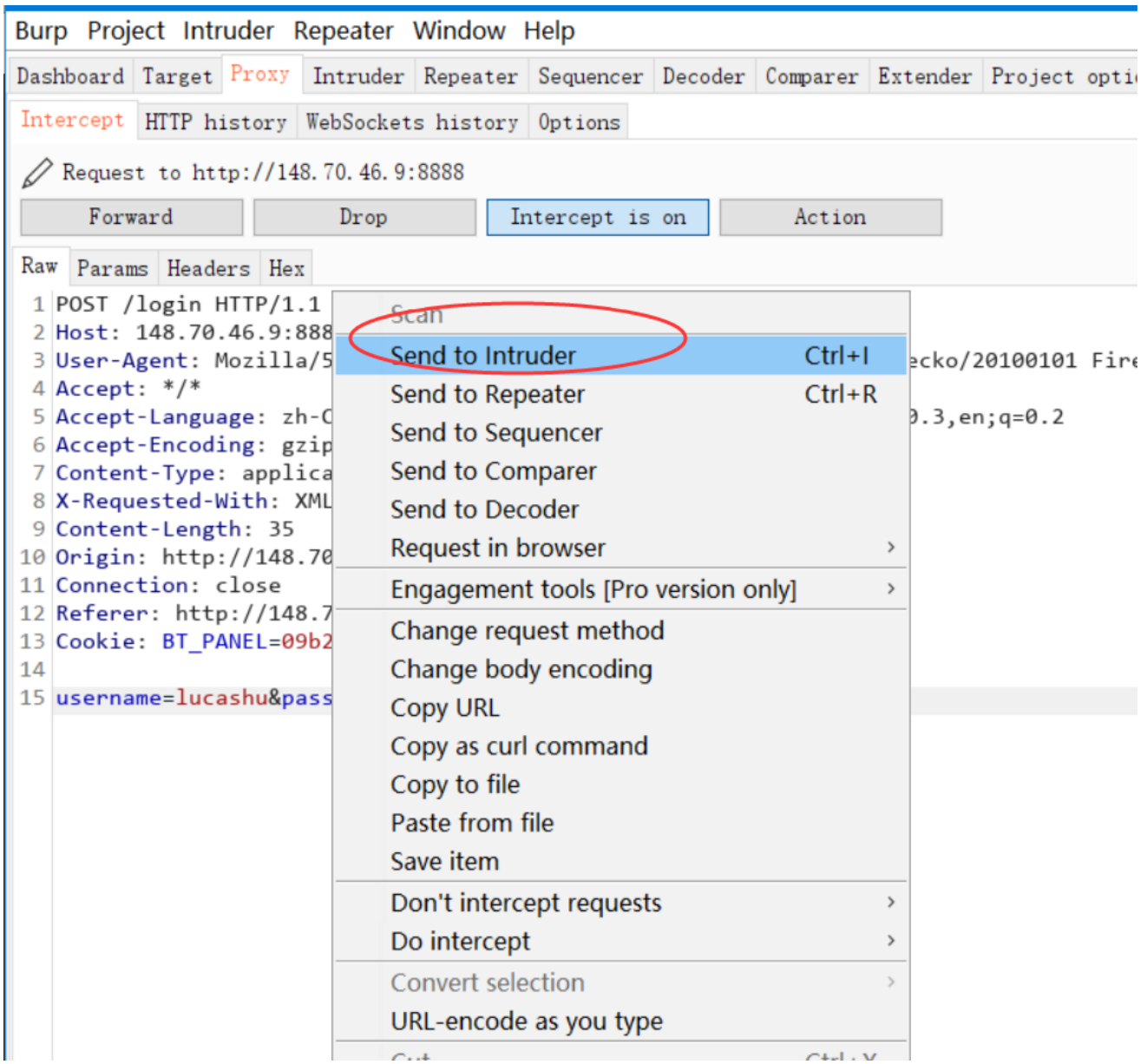
局域网设置界面，填写好代理服务器的ip和端口信息

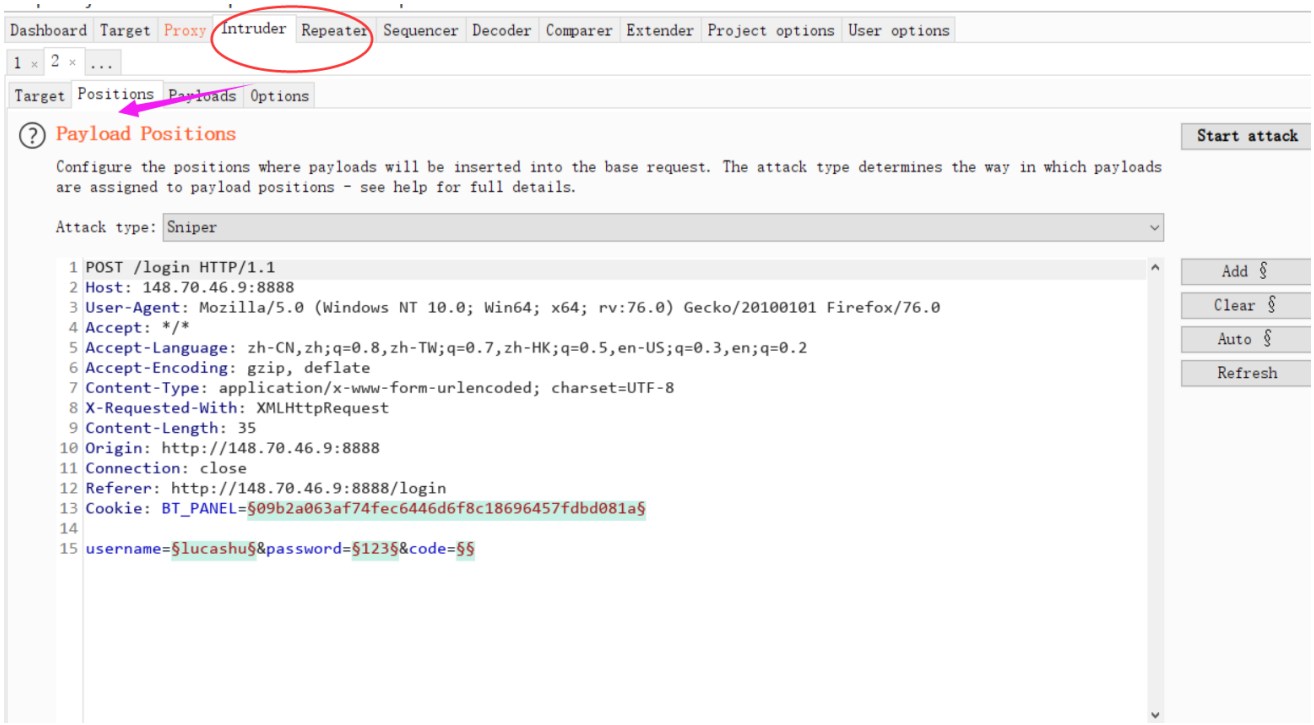
BP添加代理拦截


Burp Suite Community Edition v2020.2 - Temporary Project
urp Project Intruder Repeater Window Help
ashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Pr
Intercept HTTP history WebSockets history Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser.
as its proxy server.
Add
Edit
Remove
Running
Interface
Invis...
Redirect
Certificate
127.0.0.1:8080
Per-host
127.0.0.1:8081
Per-host
Each installation of Burp generates its own CA certificate that Proxy listeners
this certificate for use in other tools or another installation of Burp.

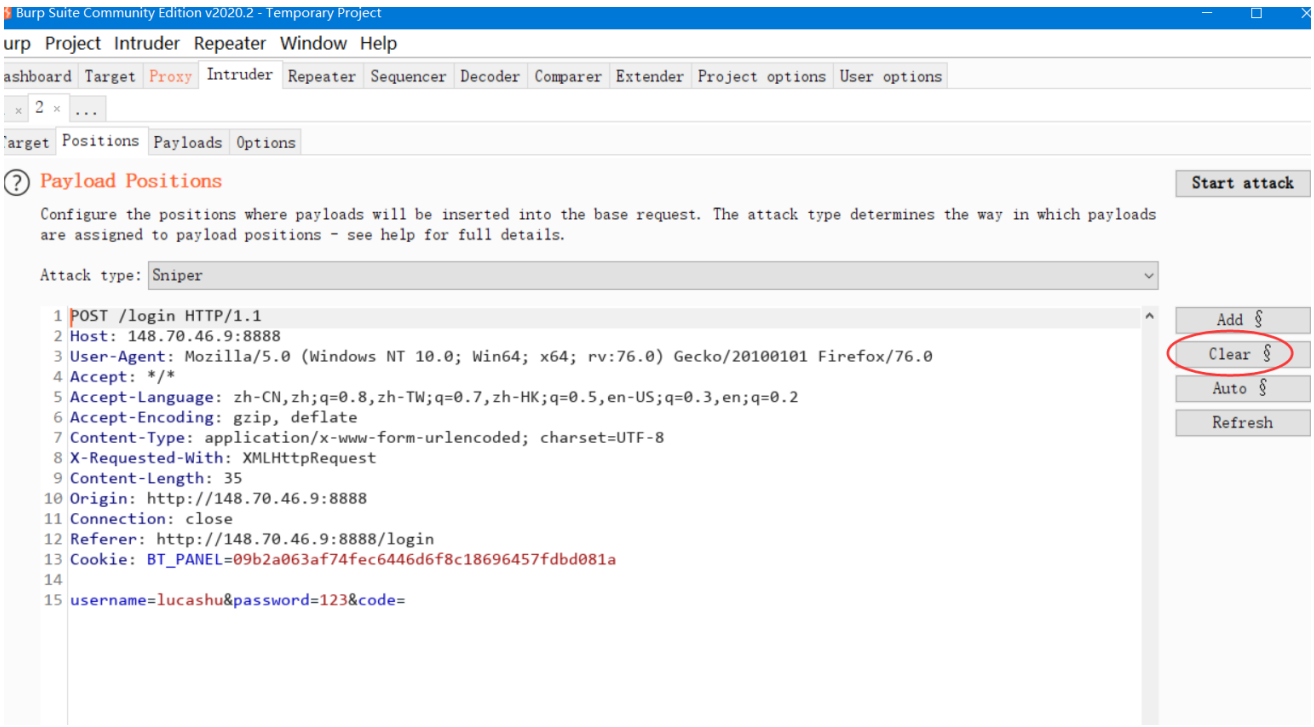

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Pr
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw
Hex

拦截登录请求


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project opti
Intercept HTTP history WebSockets history Options
Request to http://148.70.46.9:8888
Forward Drop Intercept is on Action
Raw Params Headers Hex
1 POST /login HTTP/1.1
2 Host: 148.70.46.9:888
3 User-Agent: Mozilla/5
4 Accept: */*
5 Accept-Language: zh-C
6 Accept-Encoding: gzip
7 Content-Type: applica
8 X-Requested-With: XML
9 Content-Length: 35
10 Origin: http://148.70
11 Connection: close
12 Referer: http://148.7
13 Cookie: BT_PANEL=09b2
14
15 username=lucashu&pass
ecko/20100101 Fire
0.3,en;q=0.2
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type



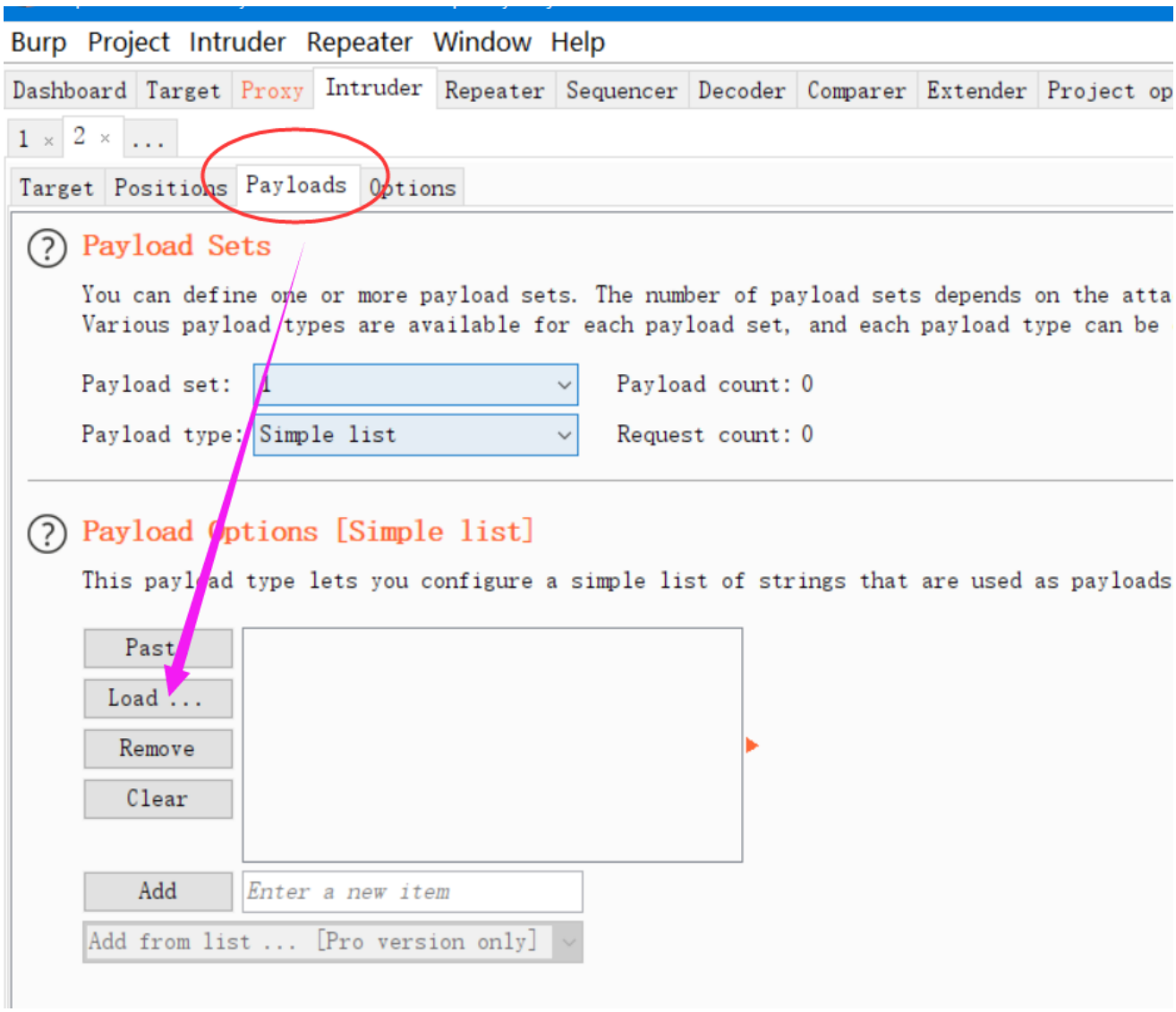
清除所有的参数



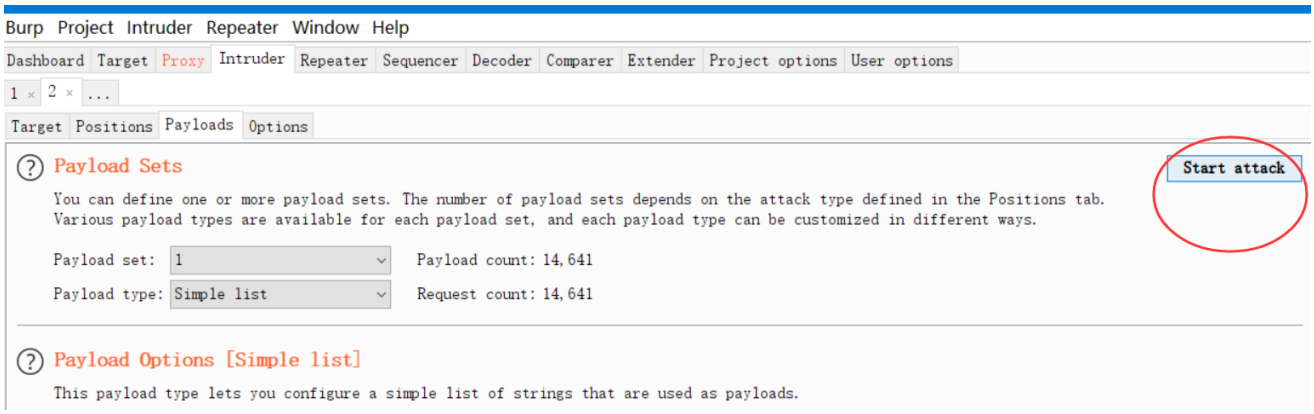
将密码添加为破解参数


get Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
1 POST /login HTTP/1.1
2 Host: 148.70.46.9:8888
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
4 Accept: */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 35
10 Origin: http://148.70.46.9:8888
11 Connection: close
12 Referer: http://148.70.46.9:8888/login
13 Cookie: BT_PANEL=09b2a063af74fec6446
8f8c18696457fdbd081a
14
15 username=lucashu&password=§123§&code=
Add §
Clear §
Auto §
Refresh

加载字典


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project op
1 × 2 × ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the atta
Various payload types are available for each payload set, and each payload type can be
Payload set: 1
Payload count: 0
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads
Past
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]

开始破解



通过比较返回参数的差异来判断正确的密码